

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

**Cyber-based C4ISR Assets:
A U.S. Air Force Critical Vulnerability**

by

John W. Neptune, Major, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lieutenant Colonel Michael Linschoten

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE APR 2009		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Cyber-based C4ISR Assets: A U.S. Air Force Critical Vulnerability				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Command And Staff College Air University Maxwell Air Force Base, Alabama				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The cornerstone of the USAF's global strike and rapid global mobility is its vast cyber-based C4ISR network. The USAF has become so dependent on cyber-based C4ISR capabilities that the network itself has truly become a center of gravity. Unfortunately, the network's critical requirements are highly susceptible to attack from a number of threats. As a result, one of the USAF's greatest capabilities has also become one of its greatest vulnerabilities. Using open-source documentation, this paper outlines the grave threat to the USAF's cyber-based C4ISR and suggests how the USAF should prepare its forces to operate in a cyber-denied environment. Current threats to the USAF's cyber-based C4ISR include traditional kinetic attack, cyberspace operations, electronic warfare, and anti-satellite weaponry; capabilities which potential adversaries have already operationalized. In light of these threats and the widespread availability and vulnerability of targets, the USAF can in no way guarantee the availability of cyber-based C4ISR on the battlefield! To mitigate this risk, the USAF must: 1) convince Airmen the threats are credible, 2) update/create cyber-related contingency plans, 3) develop and implement an extensive USAF-wide training, exercise, and evaluation program, and 4) expand its existing aggressor program. Only then will the USAF have the potential to meet the nation's strategic military goals and defend its vital national interests across the full spectrum of operations.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 41	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Disclaimer	ii
Preface	iv
Abstract	v
Introduction.....	1
Cyber-based C4ISR Assets: Critical Capability Turned Critical Vulnerability	2
Threats to Cyberspace Assets	5
Potential Adversaries	8
China	9
Russia.....	10
North Korea	11
Iran	12
The Greatest Cyberspace Threat to the USAF...Itself	13
The Way Ahead	16
Step 1: An Information Campaign.....	17
Step 2: Update/Create Installation, GCC/FCC/MAJCOM Cyber-Related Contingency Plans	17
Step 3: Develop/Implement Extensive USAF-wide Training, Exercise, and Evaluation	
Program.....	18
Step 4: Expand the Existing Aggressor Program.....	21
Conclusion	25
Appendix A: Expanded Information on Chinese and Russian Capabilities	26
China	26
Russia.....	27
Appendix B: Proposed additions to AFI 10-2501	30

Preface

Despite my background as a rated officer (KC-135 pilot), I have always been especially interested in cyberspace. During my education at Air Command and Staff College, I discovered that cyberspace is a relatively misunderstood domain. Many Airmen take cyber-based C4ISR capabilities for granted and are either unaware or unconvinced of the Air Force's overconfidence in the availability of this inherently vulnerable domain. Unfortunately, in light of growing enemy capabilities and ever-increasing dependence on cyber-based C4ISR, the Air Force can no longer afford to turn a blind eye to this critical vulnerability. If this paper serves only to increase awareness and spark further debate, it was well worth the effort.

I would like to especially acknowledge several individuals without whose assistance I may have never transcribed a single coherent thought. First and foremost, I am eternally grateful to Lt Col Mike Linschoten for looking past my inexperience in the field and allowing me to join his cyberspace seminar. He not only provided invaluable guidance and expertise throughout the year, but was also instrumental in opening my eyes to the amazing capabilities and grave threats unique to space and cyberspace. I also owe much gratitude to Lt Col Tim Franz and Major Paul Williams, who both provided me with great insight into cyberspace as well as several key inputs for this paper. I must also thank my good friend, peer, and mentor, Maj Brian Hoybach, who likely spent more time reading and re-reading my research paper than writing and editing his own...you are the man! Finally, I would like to acknowledge the ACSC staff as a whole for creating an academic environment open to discussion and innovation.

Abstract

The cornerstone of the USAF's global strike and rapid global mobility is its vast cyber-based C4ISR network. The USAF has become so dependent on cyber-based C4ISR capabilities that the network itself has truly become a center of gravity. Unfortunately, the network's critical requirements are highly susceptible to attack from a number of threats. As a result, one of the USAF's greatest capabilities has also become one of its greatest vulnerabilities. Using open-source documentation, this paper outlines the grave threat to the USAF's cyber-based C4ISR and suggests how the USAF should prepare its forces to operate in a cyber-denied environment.

Current threats to the USAF's cyber-based C4ISR include traditional kinetic attack, cyberspace operations, electronic warfare, and anti-satellite weaponry; capabilities which potential adversaries have already operationalized. In light of these threats and the widespread availability and vulnerability of targets, the USAF can in no way guarantee the availability of cyber-based C4ISR on the battlefield! To mitigate this risk, the USAF must: 1) convince Airmen the threats are credible, 2) update/create cyber-related contingency plans, 3) develop and implement an extensive USAF-wide training, exercise, and evaluation program, and 4) expand its existing aggressor program. Only then will the USAF have the potential to meet the nation's strategic military goals and defend its vital national interests across the full spectrum of operations.

Cyber-based C4ISR Assets: A U.S. Air Force Critical Vulnerability

Introduction

In 2001, President George W. Bush vowed to build a “...force that is defined less by size and more by mobility and swiftness, one that is easier to deploy and sustain, one that relies more heavily on stealth, precision weaponry and information technologies.”¹ Under President Bush’s administration, the Department of Defense (DOD) underwent a massive overhaul to create a lighter, faster, and more lethal military that leveraged technology to face increasingly dynamic threats around the world.² As a result, despite an approximate 33% cut in manpower since 1991,³ the United States military currently provides America with unmatched, full-spectrum military options to defend the nation’s vital national security interests, as demonstrated by ongoing missions in Iraq and Afghanistan, the Global War on Terrorism, deterrence in Korea, and a myriad of other contingencies across the globe.

As part of the DOD’s transformation, the United States Air Force (USAF), downsized by approximately 35% starting in 1991⁴ and realigned resources and personnel to transform into a smaller, more lethal and agile fighting force.⁵ The cornerstone of this transformation, modern technology, compensated for the significant decrease in manpower and resources by increasing overall efficiency and effectiveness. One of the USAF’s most important technological achievements is its highly-advanced and persistent Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) network. This network is also a crucial center of gravity for the present-day rapid global mobility and global attack options that the USAF brings to combatant commanders’ full spectrum of joint operations.⁶

Cyberspace (to include its associated infrastructure) is an absolutely critical requirement for the USAF’s robust C4ISR capability. Unfortunately, as noted by Secretary Gates in the 2008

National Defense Strategy, cyberspace's "unparalleled advantages" on the battlefield also present significant vulnerabilities.⁷ Due to the dynamic environment, scope, and sheer magnitude of this rapidly evolving domain, the USAF can in no way guarantee the availability of cyber-based C4ISR on the battlefield. Potential adversaries, such as nation states, non-government organizations, hackers, and terrorists, have the potential to disrupt USAF cyber-based C4ISR, significantly degrading USAF rapid global mobility and global attack capabilities.

What can the Air Force do to address the above dilemma? In the long-term, a sound solution is to: 1) build (and continually update) a redundant and secure military cyberspace infrastructure with dynamic cyber-attack/defense capabilities and 2) develop, employ, and exercise more robust continuity of operations procedures to recover from successful enemy attacks on cyber-based C4ISR. In the short-term, if the USAF continues to rely on cyber-based C4ISR as one of its "unparalleled" advantages, it must: 1) come to grips with the inherent insecurity of cyberspace and 2) take steps to mitigate the risks associated with the growing number of potential adversaries and their evolving ability to disrupt, deny, and/or degrade cyber-dependent C4ISR. *This paper analyzes why the USAF is at grave risk and suggests how the Air Force should prepare its forces to sustain operations in a cyber-denied environment.*

Cyber-based C4ISR Assets: Critical Capability Turned Critical Vulnerability

According to Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms (as amended through 17 October 2008)*, cyberspace is defined as, "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."⁸ Using this definition as a starting point, the critical requirements for the USAF's cyber-based C4ISR include both organic and joint

land, air, sea, and space-based systems (infrastructure, hardware, software) operated by civilian, DOD, U.S. Government, and international organizations. Highlights of this vast and complex network include land, sea, air and space-based military C4ISR weapon systems, personal computers, servers, mainframes, the Internet and its associated hardware/global infrastructure, non-Internet computer networks (e.g., LMR/TADL), and national and international power grids.

On the surface, these systems and their interaction are often opaque to most Airmen, but a detailed look reveals that the USAF has completely integrated cyber-based C4ISR into its full spectrum of operations. These systems support everything from command and control of combat forces (conventional and nuclear) to logistics (i.e., ordering, distributing, tracking of munitions, medical supplies, spare parts, etc.) and administration (i.e., military pay/medical records). Land, sea, air, and space-based C4ISR assets collect, store, and transmit data for operations throughout the globe. Computer systems and networks, which at first glance may seem like a luxury, store critical data, supplement and/or automate countless operational and administrative functions, and enhance communications, increasing individual and organizational effectiveness and efficiency. In short, the USAF can't operate without them! They are a key enabler for the USAF's recent reorganization, laying the foundation for lean, efficient, and streamlined processes centered on modern technology. As for the Internet, even though Airmen may not need access to "Yahoo" or "CNN" to accomplish their mission, they rely on the Internet-based Non-secure Internet Protocol Router Network (NIPRNET)/Secret Internet Protocol Router Network (SIPRNET)⁹ and their associated backbone (e.g., undersea cables, satellite links, etc.) to access and transfer vital C4ISR data on a daily basis. Finally, military and civilian power grids fuel the extensive energy needs of cyber-based C4ISR's infrastructure.

Unfortunately, several fundamental problems make it virtually impossible for the USAF to completely defend the cyber-based C4ISR critical requirements outlined above. First and foremost, as noted by Dr. Jabbour, Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, attacks on cyberspace can be extremely inexpensive, making it more cost-effective to asymmetrically deny, degrade, or destroy select U.S. capabilities than to match them.¹⁰ At the basic level, adversaries need only a computer and connection to the Internet to attack U.S. cyber-based interests world-wide.¹¹ Even more complex attacks on infrastructure, such as destroying spaced-based satellites, are significantly cheaper than researching, building, fielding, and maintaining a similar integrated capability. For example, instead of spending billions to match U.S. satellite reconnaissance capabilities, a potential adversary may simply elect to spend millions to destroy or degrade U.S. reconnaissance satellites.

Second, it is often difficult to detect attacks launched against cyberspace assets from cyberspace, let alone identify the culprit.¹² This, coupled with jurisdictional concerns, presents the USAF with a myriad of challenges and roadblocks when dealing with cyber-espionage and/or cyber-attacks.¹³ For instance, how can the USAF respond to an unseen foe? Can it justify retaliation without convincing evidence? Could retaliation cause further adverse impacts to the USAF, other government agencies, or allies?

Finally, due to the vast size and scope of cyberspace, adversaries can choose from and exploit seemingly limitless critical vulnerabilities, making it cost-prohibitive to provide an all-encompassing defense. At best, the United States can, in the words of Dr. Jabbour, “attempt to anticipate and avoid threats, detect and defeat threats, [and] survive and recover from attacks.”¹⁴ Preventing successful attacks altogether, on the other hand, is not only cost-prohibitive, but also

technologically unfeasible. As a result, the aforementioned cyber-based C4ISR critical requirements are also exposed critical vulnerabilities. Regrettably, many of the people who seem to understand this concept also happen to be potential adversaries.

Threats to Cyberspace Assets

To make matters worse, not only can adversaries exploit multiple cyber-based C4ISR vulnerabilities, they have several distinct capabilities to choose from when making an attack. Principal offensive capabilities include, but are not limited to, cyberspace operations, electronic warfare (EW), traditional kinetic attack, and more advanced, but evolving, anti-satellite weapons (ASAT). The brief summary of capabilities that follows is not intended to discuss threats in detail, nor to imply whether or not the United States has similar capabilities, but rather to outline the inherent vulnerability of the USAF's cyber-based C4ISR.

Cyberspace operations, which JP 1-02 defines in part as, "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace,"¹⁵ is one of the most cost effective ways to degrade the USAF's cyber-dependent C4ISR. Using a single computer connected to the Internet or, worse yet, a compromised computer within the military network, "hackers" can potentially access critical systems. Once in, they can unleash malicious software, such as viruses or worms, which spread throughout and corrupt networked systems, causing anything from simple system degradation or denial of service to the destruction of data and/or hardware.¹⁶ More skilled "hackers" can tamper with critical systems by modifying data and/or reprogramming/replacing/adding code that could disrupt, deny, or degrade critical C4ISR capabilities.¹⁷ The method "hackers" use is largely irrelevant, since the end result is the same...disruption, denial and/or degradation of cyber-based C4ISR capabilities. For example, a successful cyber-attack on United States Transportation

Command's or Air Mobility Command's unclassified logistics networks or infrastructure could have far reaching primary, secondary, and/or tertiary effects. What would happen if the wrong munitions, medical supplies, or replacement parts were sent overseas to one of the USAF's expeditionary wings due to a "software glitch?" What if critical logistics systems simply "crashed?" What if this was just one of many parallel attacks against the USAF's C4ISR assets? Would it affect the combat readiness or capabilities of a combatant commander's forces? Could it affect the USAF's ability to meet strategic military goals or defend vital national interests?

Another way to disrupt, deny, or degrade cyber-dependent C4ISR assets is EW, or, more specifically, electronic attack (EA). JP 1-02 defines EA as the "division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability."¹⁸ Adversaries could use electromagnetic pulses (EMP) or electromagnetic jamming to disrupt the flow of information through cyberspace (i.e., communications satellites, GPS satellites, etc.), effectively neutralizing the critical C4ISR capabilities these systems would normally deliver. Several potential adversaries already possess nuclear weapons, which can create large EMPs; and conventional variants are technologically feasible.¹⁹ Jamming, unlike EMP/ASAT weaponry, is not rocket science (pun intended). One need only perform a basic search on the Internet to find ads for commercial cell phone jammers, radar jammers, and laser jammers. While they do not necessarily affect military equipment, they are indicative of the relatively simple technology needed to field basic electromagnetic weapons. In reality, multiple nations field more expensive and complex military variants that could have a significant impact on critical land, sea, air, and satellite-based C4ISR capabilities. Once again, this should raise serious concerns. For instance, could the USAF, which relies on centralized command and

decentralized execution, operate efficiently without its normal array of communications? What would happen to combat effectiveness without the GPS constellation, which has become a key component of precision attack, navigation, and command and control? As with cyberspace operations, could EW alter the balance of power and affect the USAF's ability to meet strategic military goals or defend vital national interests?

The third means to neutralize cyber-dependent C4ISR assets is traditional kinetic attack. Using tried and true technology, such as bullets, missiles, or bombs, adversaries could destroy key nodes in the cyber-based C4ISR infrastructure, once again disrupting, denying, and/or degrading vital USAF cyber-based C4ISR capabilities. The unexpected loss of Internet capacity in the Middle East in 2008 perfectly illustrates the potential for kinetic attack. Approximately 90% of Internet traffic to the Middle East runs through a system of undersea cables, while satellites process the remaining 10% of Internet traffic. So, when unknown events damaged several of the Middle East's undersea fiber-optic cables in short succession in early 2008, the resulting loss in Internet capacity adversely affected over 80 million users in the Middle East, Africa, and Asia.²⁰ Although this did not completely cutoff Internet communications in the region or necessarily affect military operations in United States Central Command, the situation shows that cyberspace has tangible vulnerabilities that, when acted upon, can produce undesirable effects. This shows that potential adversaries can physically attack key nodes (critical requirements) in the USAF's C4ISR infrastructure, such as joint/coalition air operations centers (JAOC, CAOC), ground-based Air Force Space Command satellite command and control centers, and satellite relay stations. What would happen if an adversary severed the communications cables to a combatant command's JAOC/CAOC? Would there be enough redundant satellite and radio-based systems to ensure adequate C4ISR for USAF assets? What if

an adversary bombed a JAOC/CAOC or satellite command and control center? Could it affect the USAF's ability to meet strategic military goals or defend vital national interests?

The final method adversaries could use to neutralize USAF cyber-dependent C4ISR assets is ASAT weaponry, which destroys or neutralizes satellites orbiting Earth. Contrary to common perception, these weapons are not new; the Soviet Union successfully tested the first ASAT weapon in 1968, which spurred a flurry of research by both the United States and Soviet Union for the next several decades.²¹ During this period, both nations researched multiple ASAT systems (co-orbital, direct-ascent, directed energy, and electronic interference) with varying degrees of success.²² Today, even though the United States, Russia, and China are the only nations that have successfully tested operational systems, the technology required to build ASAT weapons is less complex and easier to procure than one would think.²³ Thus, this begs the question...could the USAF operate effectively without the extensive network of satellites and their associated C4ISR capabilities? Could the loss of key satellite capabilities affect the USAF's ability to meet strategic military goals or defend vital national interests?

The bottom line: USAF cyber-based C4ISR is dependent upon a vast network of assets that includes land, sea, air, and space-based components. The complexity and interdependency of this network, coupled with a growing number of threats, creates too many avenues of attack to mount an impenetrable defense. Consequently, adversaries may be able to disrupt, deny, and/or degrade critical cyber-based C4ISR capabilities, if only for a short, albeit crucial, time, affecting the USAF's ability to meet strategic military goals and/or defend vital national interests.

Potential Adversaries

A discussion on potential threats is merely an academic exercise without matching vulnerabilities and threats with adversaries that have both the capabilities and the will to use

them. Currently, the most notable threats are China, Russia, North Korea, and Iran (note: since traditional kinetic attack is commonplace, this section will not cover enemy capabilities in this category). See Appendix A, Capabilities of Potential Adversaries, for more detailed information on China and Russia.

China

According to the Department of Defense's *Annual Report to Congress on the Military Power of the People's Republic of China 2008*, China is "pursuing comprehensive transformation from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short duration, high intensity conflicts along its periphery against high-tech adversaries – an approach that China refers to as preparing for 'local wars under conditions of informatization.'"²⁴ Although this transformation initially appears to be aimed at a potential conflict over Taiwan, Department of Defense officials suggest China is planning for the future as well, essentially preparing its military for future conflicts over resources and/or territories.²⁵ Fully aware that it currently can't compete symmetrically against U.S. military forces, the cornerstone of China's new strategy is increasingly focusing on anti-access strategies with a large emphasis on space and cyberspace.²⁶ China's buildup of cyber forces/capabilities, procurement of EW systems, and successful development of ASAT weaponry, mark China as one of the greatest threats to the USAF's cyber-based C4ISR.

China's cyber attack capabilities are mature, backed by cyberwarfare doctrine, a cyberwarfare training program for officers, and integrated cyberwarfare field training.²⁷ Suspected cyber capabilities include, but are not limited to: large, advanced BotNets, non-nuclear electromagnetic pulse weapons, a zero-day exploitation framework, compromised counterfeit computer hardware, peripheral devices, microprocessors, and software, advanced

dynamic exploitation options, wireless communication jammers, computer logic bombs, viruses and worms, and cyber data collection tools.²⁸ As for EW, China could use its existing nuclear munitions to create EMPs and has operational ground-based EW satellite jammers to degrade U.S. communications satellites.²⁹ With regards to space, China demonstrated an operational capability to attack low-Earth orbit satellites in 2007.³⁰ Whether or not they are pursuing, or already have, the capability to intercept satellites at higher orbits with kinetic ASATs is unclear. Finally, as noted by the Department of Defense, the Chinese are aggressively pursuing directed-energy weapons (e.g., lasers).³¹ If perfected, the Chinese could combine these two technologies to mount a grave threat to a variety of U.S. satellites.

Bottom Line: China already possesses the doctrine and proven kinetic (traditional military), cyber, EW, and ASAT systems to infiltrate and/or attack U.S. cyber-based C4ISR assets. Additionally, given its tendency to supply military aid to other nations, China will likely export some, or all, of these technologies to other potential adversaries.

Russia

Despite the breakup of the Soviet Union, Russia remains a highly-capable military power that has recently showed renewed signs of life. As of 2008, Russia had increased defense spending approximately 500% over 2002 expenditures,³² and still controlled over 900 nuclear delivery devices and 4200 nuclear warheads.³³ In recent shows of force, the Russian military revived bomber patrols near Alaska in 2007³⁴ and is actively projecting military power in South America with the help of Venezuela, which has given safe haven to Russian warships³⁵ and aircraft since 2008.³⁶ As relations continue to cool, renewed military competition, or even conflict, is more plausible than ever. With a wide array of modern cyberwarfare capabilities and advanced Cold War technology, Russia presents a credible threat to cyberspace assets.

According to defensetech.org, Russia's suspected offensive cyberwarfare capabilities include: large, advanced BotNets, non-nuclear electromagnetic pulse weapons, compromised counterfeit computer software, advanced dynamic exploitation options, wireless communication jammers, computer logic bombs, viruses and worms, and cyber data collection tools.³⁷ As with China, Russia could also use its nuclear munitions to create EMPs. In addition, Russia possesses a growing number of conventional EW options, having greatly expanded Cold War-era EW capabilities to support military operations during the Second Russia-Chechen War.³⁸ Last, but certainly not least, Russia has access to several proven kinetic ASAT systems from the Cold War and a legacy of research and development for other kinetic and directed energy systems.³⁹

Bottom Line: Russia maintains proven kinetic (traditional military), cyber, EW, and ASAT systems that can infiltrate and/or attack U.S. cyber-based C4ISR assets. Russia will likely offer these capabilities to other potential adversaries given its historic tendency to export military arms.

North Korea

North Korea and the United States have been in an uneasy truce for over half a century. Although the communist regime is essentially isolated from the world community, it has a relatively large and capable conventional force. Advances over the past decade underscore a doctrinal shift that is focusing evermore on asymmetric capabilities, especially with regards to cyberspace and ballistic missile technologies.

North Korea's suspected cyberwarfare capabilities include: moderately-advanced distributed denial of service capabilities, and moderate virus/malicious code capabilities.⁴⁰ Its EW capabilities are not well publicized and are likely rudimentary (e.g., basic jamming),⁴¹ but the fact that China, North Korea's neighbor and chief benefactor, possesses more advanced EW

capabilities increases the likelihood that North Korea could field more advanced EW systems. In addition, as a fledgling nuclear power, North Korea may soon be able to field nuclear munitions to create EMPs. North Korea does not currently have an operational ASAT system, nor is it officially developing one. However, its recent declaration that it is pursuing a space program,⁴² coupled with existing short-range, medium range, and intermediate range ballistic missile technology,⁴³ signify that kinetic ASAT systems are a distinct possibility in the not-too-distant future.

Bottom Line: North Korea currently fields basic kinetic (traditional military), cyber, and EW (likely) capabilities that are a credible threat to USAF cyber-based C4ISR assets. Moreover, the fact that this long-time foe, which has close ties with China, has started to deliberately delve into this domain is a reason for concern.

Iran

Over the past several years, Iran has increased hostile overtures towards the United States, which is likely an attempt to increase popular support for regional policies and ambitions.⁴⁴ Since the U.S.-led invasion of Iraq, Iran has been concerned by the prospect of combat with the highly-advanced and digitized U.S. military. As a result, Iran has taken steps to acquire sophisticated weaponry, focusing on weapons of mass destruction precursors, advanced conventional systems, and digital/information technology,⁴⁵ which could significantly strengthen its ability to wage a successful asymmetric warfare campaign.

Iran has a growing cyberwarfare inventory that currently includes: compromised counterfeit computer software, wireless data communications jammers, computer viruses and worms, cyber data collection exploits, computer and networks reconnaissance tools, and embedded Trojan time bombs.⁴⁶ Although there is no evidence Iran has significant EW

capabilities, Russia, one of Iran's chief suppliers,⁴⁷ could easily change the situation. Iran may not have ASAT systems, but its recent satellite launch on February 3, 2009,⁴⁸ puts it one step closer to developing kinetic ASATs. Furthermore, if Iran successfully perfects a nuclear weapons program, it will also gain the ability to produce nuclear EMPs.

Bottom Line: Like Korea, Iran's kinetic (traditional military), cyber, and EW (likely) systems are a credible, albeit limited, threat to the USAF's cyber-based C4ISR assets. Military exchanges between Iran/Russia and Iran/Korea increase the possibility that Iran may develop additional methods to asymmetrically dampen U.S. military's capabilities in the region.

The Greatest Cyberspace Threat to the USAF...Itself

Potential adversaries, such as China, Russia, North Korea, and Iran, recognize cyber-based C4ISR as a center of gravity...they recognize cyberspace as a critical vulnerability...if necessary, they will exploit this vulnerability...and if the USAF isn't fully prepared, the consequences could be disastrous. Based on potential threats and the futility of an all-encompassing defense, the USAF must be prepared to operate in a cyber-denied environment. Ironically, the greatest obstacle to avoiding disaster is the USAF, which has not sufficiently addressed the threat to cyber-based C4ISR. To break the overconfidence in cyber-based C4ISR, the USAF must change its culture and acknowledge the gravity of the situation.

The first step in managing this culture change is to identify the root of the problem. Has the USAF's senior leadership, who began their careers before the explosion of cyber-based C4ISR, not grasped the reliance on, overconfidence in, threat to, and vulnerabilities of cyber-based C4ISR? No... there is little doubt that the USAF's senior leaders understand what is at stake, but they only account for a very small percentage of USAF personnel. The problem lies with the younger generations of Airmen (which include lower and mid-level leadership), who

have relied on modern technology their entire careers. Since the late 1990s, the USAF has integrated computer/information-based technology in newer and more advanced weapons systems on the battlefield as well as in the workplace. For instance: over the past decade, electronic mail has replaced the telephone as the primary means of service-wide communication; Internet-based collaborative tools, such as the USAF's Knowledge Know, are centralizing and integrating professional forums and expertise; recent years have witnessed an explosion in reliance on unmanned aerial systems (UAS) for Intelligence, Surveillance, and Reconnaissance and precision attack (today, the USAF maintains a current fleet of approximately 110 MQ-1 Predators,⁴⁹ 10 MQ-9 Reapers,⁵⁰ 10 RQ-4 Global Hawks,⁵¹ and a classified number of RQ-11 Ravens⁵²); pilot trainees now conduct training in state-of-the-art glass cockpit aircraft, focusing not only on basic airmanship, but ever more on technological enhancements; and finally, precision guided-munitions, once a novelty, are the absolute weapon of choice. A complete list of technological advances would be unnecessarily extensive, but suffice it to say that the USAF has integrated cyber-based C4ISR technology into all aspects of operations, and tech-savvy Airmen have been all too happy to exploit this technology to the fullest.

What is absolutely astounding, however, is how Airmen, who absolutely rely on modern technology, are so seemingly confident in the security, integrity, and availability of cyber-based C4ISR, especially given the threats noted above. For example, large numbers of Airmen seem more concerned with the 'hassles' presented by protective measures than they are with actually protecting critical cyber-based C4ISR capabilities. When the USAF began filtering the websites Airmen could access from government computers (e.g., AOL, Hotmail, blogs, etc.), there was widespread outrage; and when USAF leadership decided in late 2008 that Airmen could no longer connect portable hard drives, USB "thumb drives," or similar hardware to government

computers, Airmen openly questioned both the necessity and sanity of such a move. It spurred a series of spirited debates that highlighted a substantial operational impact from a technology that didn't even exist several years ago. In fact, each time the USAF implements increased security measures, the reaction is similar...large numbers of Airmen, who don't seem to quite grasp the strategic situation, begrudgingly accept the new rules, then often try and find ways around them.

What could possibly fuel this seemingly blatant disregard for security? Are the younger generations of Airmen so enamored with technology that they are ready and willing to dismiss credible threats to cyber-based C4ISR? Have Airmen lost confidence in the higher headquarters' ability to understand this issue? No, on both accounts. This paper suggests the answer is actually quite simple...many Airmen are simply ignorant of the threat. Over the past decade, the USAF (and other government agencies) has actually done itself a great disservice. Instead of briefing all personnel to their appropriate security clearances, the USAF has kept the developments in cyberspace a quiet secret. Even if it chose to brief personnel on current threats and operations, the USAF has classified much of the key information so high that it wouldn't make it down to the majority of Airmen in the first place. The closest thing to a comprehensive mass training and education program that outlines threats and vulnerabilities is the current IA training program, which only shallowly discusses hostile cyberspace operations (but not EW, kinetic attack, or ASATs). Sadly, to underscore the inadequacy of this program, many Airmen complete this basic computer-based course, which only covers very rudimentary concepts, in less than 20 minutes. It does not cover the threats, vulnerabilities, and resulting operational deficiencies in near enough detail...and it is completely unclassified. While it is understandable that the USAF must maintain a measure of security to protect collection sources, intelligence capabilities, and organic cyber defense capabilities, it simply can't afford to keep the majority of

Airmen, who are “on” the ‘battlefield,’ in the dark. *Every Airman* that logs on to a computer, works on a C4ISR weapon platform, or is stationed at a base that has, supports, or uses cyber-based C4ISR infrastructure is already “on” the ‘battlefield’ and clearly has the need to know!

So, even though cyber-based C4ISR is such an integral part of USAF operations, it is easy to see why many Airmen simply don’t believe potential adversaries can disrupt, deny, and/or degrade cyber-based C4ISR capabilities; there currently isn’t a consolidated effort to convince them otherwise. Yet, since every Airman is a combatant in the cyberspace domain, the USAF must make a universal and concerted effort to reverse this disturbing trend. Would Airmen be ready to fight through a chemical or biological attack today if they didn’t believe the threat was real? Would they take their training and precautionary measures seriously? Probably not. Would the Airmen manning the nation’s strategic missile silos during the Cold War have been as disciplined, well-prepared, and motivated if they had never believed in the Soviet threat? Not likely. Airmen must understand and believe in the threat to maximize current defense postures in the event enemy forces compromise cyber-based C4ISR.

The Way Ahead

Thus far, this paper has outlined a grim situation. The USAF has become dependent on a center of gravity that is extremely difficult to defend; potential adversaries have identified this weakness and are preparing to exploit it; and, worst of all, many of the Airmen who depend on cyber-based C4ISR are largely unaware of and unprepared for the growing threats. Fortunately, it is not too late to address this alarming trend. If the USAF acts quickly and aggressively, it can effectively prepare its forces to operate in a cyber-denied environment. To do this, the USAF must: 1) convince Airmen the threat is real, 2) posture the USAF to deal with attacks by updating/creating installation, Geographic Combatant Command (GCC), Functional Combatant

Command (FCC), and Major Command (MAJCOM) cyber-related contingency plans, 3) develop and implement an extensive USAF-wide education, training, exercise, and evaluation program, and 4) expand its existing cyberspace aggressor program.

Step 1: An Information Campaign

Luckily, convincing Airmen that the threat to cyber-based C4ISR may be easier than it sounds. First and foremost, the USAF must bring Airmen up to speed on the entire situation *commensurate with their security clearances*...and it must do this immediately. As cyber-based C4ISR users and/or operators, every Airman is not only a link in the USAF's defensive armor, but a potential chink as well; as such, all Airmen have a "need to know." Second, until incorporated into a formal education and training program, the USAF should implement mandatory recurring (recommend quarterly, minimum) situation briefings to keep the force focused and informed on developments in this dynamic domain. These briefings should focus on new capabilities, threats, and vulnerabilities while covering updates on documented cyber-based C4ISR attacks and methodology. Keeping the entire force apprised of developments will help foster a culture of vigilance, to include a renewed emphasis on OPSEC, rather than a culture of blind trust. Finally, USAF leadership should reevaluate the classifications of known threats, capabilities, vulnerabilities, and ongoing attacks to balance the need for secrecy with Airmen's need to understand the situation. In the end, this should help Airmen develop the right frame of reference and state-of-mind to recognize and break the overconfidence in cyber-based C4ISR.

Step 2: Update/Create Installation, GCC/FCC/MAJCOM Cyber-Related Contingency Plans

Once the USAF brings Airmen up to speed on the current situation, the next step is to focus on basic contingency planning requirements. Unfortunately, in the draft 5 Feb 08 DOD Inspector

General Report on *Contingency Planning for DOD Mission-Critical Information Systems* is indicative of the overall situation, this may be difficult. According to the draft report, the DOD IG projected that the owners of 68 of the USAF's 85 mission-critical systems "...did not develop or could not provide evidence of..." required contingency plans.⁵³ More importantly, the DOD IG also projected that none of the USAF's 85 mission-critical systems owners tested or could provide evidence of testing for the required contingency plans⁵⁴ that are supposed to protect the "...availability, integrity, authentication, confidentiality, and nonrepudiation of a system's information."⁵⁵ This highlights a significant deficiency in contingency planning and exercising that may very well be a significant problem throughout the entire USAF.

Consequently, the USAF should take this opportunity to perform a thorough assessment of not only Information Systems contingency plans (critical and non-critical), but all USAF-wide contingency plans related to cyber-based C4ISR capabilities. The purposes of this assessment should be to: 1) ensure compliance with DOD and USAF regulatory guidance, 2) review existing contingency plans and identify/correct shortfalls, and 3) build required contingency plans not yet on file. This will help bolster the USAF's ability to meet the NMS-CO mandated "ability to operate through degradation" by taking into account "resilience, redundancy, restorative capacity, consequence management, [and] continuity of operations (COOP)..."⁵⁶ in cyberspace.

Step 3: Develop/Implement Extensive USAF-wide Training, Exercise, and Evaluation Program

With the exception of the generic IA and Operational Security programs, the USAF does not currently execute a widespread, consolidated education, training, and exercise program that addresses attacks on cyber-based C4ISR. Even strategic exercises, such as the Future Capabilities Games and Eligible Receiver, and operational exercises, such as Red Flag, Virtual

Flag, Blue Flag, Black Demon, and the proposed “Cyber Flag” (dedicated cyberspace operations exercise proposed by Maj Hansen in 2008), only include a limited number of Airmen with specific skill sets and specialties. Moreover, the USAF often limits simulated attacks on cyber-based C4ISR during many of these exercises to prevent interference with ‘more pressing’ objectives.⁵⁷ At best, current programs prepare cyber-based C4ISR defenders and infrastructure operators with the skills, training, and experience necessary to recognize and recover from enemy attacks, but they do not prepare the majority of everyday Airmen (cyber-based C4ISR users) for operations in a contested cyberspace environment.

To put the general education, training, exercise, and evaluation deficiency into perspective, compare the IA training program with the biological, chemical, nuclear, and radiological attack (collectively referred to as weapons of mass destruction—WMD⁵⁸) readiness. Despite relatively widespread availability, not a single nation has ever used WMD against the United States; the U.S. response and international consequences for such an attack would most likely be severe. Yet, the mere fact that potential adversaries have the capability to field WMD has prompted the USAF to establish the Air Force Emergency Management (EM) Program, which ensures all Airmen can “prepare for, prevent, respond to, [and] recover from” chemical, biological, radiological, nuclear, and high-yield explosive attacks.⁵⁹ As a part of this program, every USAF unit must “develop plans, training, contingency response checklists and exercises based upon a realistic threat and assessment of resources that will be available in a contingency.”⁶⁰ The majority of Airmen must complete both web-based training and local classroom and demonstration training, while installations plan and execute multiple recurring, realistic exercises that “embody the ‘train the way we fight’ concept” and “validate actual plans, policies, procedures, processes, and doctrine.”⁶¹ Inspector General teams even evaluate these

procedures during Operational Readiness Inspections, grading the “ability to survive and operate (ATSO)” for installations with wartime or contingency missions.⁶² Thus, in stark contrast to the narrow audience that train for attacks against cyber-based C4ISR, the USAF has gone through great lengths to educate, train, and prepare Airmen for a WMD attack that hasn’t materialized in over half a century.

The most timely, efficient, and effective way to correct this deficiency is to integrate cyber-based C4ISR attack into the USAF EM Program. The EM Program already provides: 1) “...higher headquarters, installations, and unit commanders with the policies, guidance, structure, and roles and responsibilities to prepare for, prevent, respond to, recover from, and mitigate threats to their mission” and 2) the “guidance to plan, conduct, and evaluate Air Force EM exercises.”⁶³ Instead of creating an entirely new program from the ground up, the USAF could incorporate education, training, exercise, evaluation, and frequency requirements and standards into the EM program’s proven template. These new courses, exercises, and evaluations would give Airmen the background knowledge, skills, and experience necessary to, as noted earlier, “operate through degradation.” At a minimum, cyber-based C4ISR additions to the EM program should include: 1) a basic cyberspace orientation course for all Airmen, 2) a recurring cyberspace defense awareness course for all Airmen, 3) realistic installation-wide cyberwarfare exercises, and 4) realistic GCC/FCC/MAJCOM-wide cyberwarfare exercises.

The basic cyberspace orientation would be a one-time course that introduces cyberspace and its associated C4ISR capabilities to all new Airmen (commensurate with security clearances). Ideally, Airmen should attend this course shortly after basic training (i.e., tech schools, pilot training) since cyber-based C4ISR will be part of their lives from the start. At a minimum, course content should include those items listed in Appendix B.

Unlike the generic orientation course, the cyberspace defense awareness should cover more specific and tailored education and training based on an installation's/organization's mission (commensurate with security clearances). Airmen should initially take this course upon arrival at a permanent duty station (for PCSs) or a TDY location (AEF deployments), then recurrently based on Appendix B. Course content should include items in Appendix B.

Proposed additions to the EM program should also include multiple installation and GCC/FCC/MAJCOM-wide exercises that simulate realistic attacks to cyber-based C4ISR (100% organization participation). This will give installations, GCCs/FCCs/MAJCOMs, and the IG (ORIs) the opportunity to test and evaluate cyber-based C4ISR vulnerabilities, contingency plans, readiness, etc. Appendix B outlines proposed exercise scenarios, participants, content, and frequencies. And yes, exercise frequencies may seem aggressive, but the threat to cyber-based C4ISR is too great to accommodate mere convenience. However, to mitigate this inconvenience, installations and GCCs/FCCs/MAJCOMs could align these exercises with HHQ exercises and/or other operational exercises to reduce the drain on available time and resources. The USAF would also need to provide additional IG manpower, expertise, and funding for ORIs. In light of decreasing budgets this may be daunting, but the USAF must make a serious investment in this process to guarantee its ability to meet strategic military goals and defend vital national interests.

Step 4: Expand the Existing Aggressor Program

Last, but certainly not least, the USAF needs to bolster its existing cyber aggressor program. Currently, Airmen from the 57th and 177th (ANG) Information Aggressor Squadrons infiltrate DOD networks world-wide to: 1) test cyber-defenses, attack recognition, and response and recovery actions/procedures, 2) identify shortfalls and gaps in defenses, and 3) assist friendly forces in developing new strategies and systems to prevent future attacks.⁶⁴ The intent of this

program, dubbed the Information Operations Road Show, is to train Airmen to recognize and recover from attacks by simulating operations against friendly forces using known threats.⁶⁵ To kick off an “attack,” the “Aggressors” spend months remotely and covertly infiltrating systems to gain a foothold in cyberspace at the targeted installation.⁶⁶ Next, the “Aggressors” send a team to the field, which exploits OPSEC deficiencies⁶⁷ to defeat the installation’s layered defenses and gain “long-term, unhindered access” to key mission-related information.⁶⁸ Finally, the “Aggressors” replicate the simulated attack for the installation commander and staff, providing both positive and negative feedback that ultimately improves friendly defenses.⁶⁹

This is a highly effective training program, but falls well short of simulating realistic, unexpected enemy attacks since the “Aggressors” typically do not disrupt, deny, and/or degrade cyber-based C4ISR capabilities that physically affect a base’s mission or operations; but, not without reason. The “Aggressor” squadrons do not have the manning or funding to provide this additional dimension.⁷⁰ In addition, disrupting, denying, and/or degrading real-world C4ISR capabilities can create potentially unsafe situations.⁷¹ Finally, current USAF culture is more comfortable with showing off strengths than revealing vulnerabilities; commanders are not necessarily enthusiastic about revealing a base’s inability to defend vital assets.⁷²

In reality, the Information Operations Road Show simulates “cyber-espionage” and intelligence preparation of the battlefield more than actual “attacks” against USAF cyberspace assets. It does not give your everyday, run-of-the-mill Airmen at “Base X” an opportunity to train for, let alone recognize, a major attack against cyber-based C4ISR. For instance, would a successful attack against cyber-based C4ISR capabilities for Air Mobility Command’s Tanker Airlift Control Center (TACC) and select wings degrade rapid mobility; if so, how much? Could TACC manage its world-wide fleet with an unexpected and long-term loss of

NIPRNET/SIPRNET and/or associated data? Could secondary power systems feed vital assets at length if enemy forces took out the local power grid? How long would it take Airmen (network defenders, Airman on TACC's "floor," aircrew) to notice that an enemy had inserted malicious code into fleet management and command and control software? Can the USAF afford to wait for an actual attack to find out? One could apply similar questions to any base or mission, and answers would be equally as disconcerting; the potential for disaster is alarming.

To make matters worse, time and geography, once one of the USAF's closest allies, mean little in cyberspace. There will likely be little or no warning for pending attacks against the USAF's cyber-based C4ISR assets. Preparation is: 1) covert in nature (i.e., sabotage), 2) relatively quick (i.e., ASAT, jamming), or 3) a combination of the two (i.e., attacks through cyberspace...attacks based in cyberspace are especially dangerous; a cunning enemy will disguise preparation as mere espionage, and when the actual attack begins, it will occur at up to two-thirds the speed of light⁷³). Consequently, Airmen, who represent the first line of defense for cyber-based C4ISR, should get used to the fact that an attack can happen in an instant; they need to understand attacks will probably be widespread and have far reaching effects; and, they must be ready to operate indefinitely without the normal array of cyber-based C4ISR assets.

Providing Airmen with more realistic training is an optimal way to do this. Several current programs, such as Red Flag, Virtual Flag, and Blue Flag, already provide excellent cyberwarfare training, but the target audiences are not nearly large enough given the strategic situation. The Information Operations Road Show, on the other hand, has the potential to capture a much larger audience (in their natural work environment). To fully capitalize on the "Aggressor" program, the USAF should divert more resources (manpower and money) to these units. Funding may be scarce, but the USAF can't afford to lag behind in establishing continuity

of operations for cyber-based C4ISR, which, as noted earlier, truly is a USAF center of gravity. Second, “Aggressors” must have backing from the chain of command to simulate attacks against cyber-based C4ISR assets, even if they affect an installation’s or organization’s missions and associated operations...*no matter how inconvenient.*

Will this increase the risk for a safety incident? Yes, but the USAF has been doing this for years. For example, aircrew members have been simulating airborne emergencies and associated procedures for decades (e.g., simulated forced landings, engine failures, etc.). However, the flying community has levied set rules of engagement (ROE) to mitigate the risk associated with this training. With well-planned ROE, the USAF could similarly mitigate the risk associated with more robust “Aggressor” attacks while providing Airmen realistic training. For instance, if “Aggressors” infiltrate “Base X” and acquire the information and permissions needed to “take down” a wing command post or base operations, let them. No, they don’t have to actually shut down systems to make the point. Simply showing up at a command post or base ops desk and informing personnel that they have lost “X, Y, and Z” until further notice would suffice (assuming “Aggressors” could prove ability to take down the system). In the event of an actual emergency (airborne or on the installation), command post or base ops personnel would of course be allowed to resume normal operations following appropriate responses. As another example, “Aggressors” could walk over to the base tower and tell air traffic controllers that enemy forces have successfully jammed communications. Let the controllers send out an exercise notification, but leave it at that, except, once again, in the event of an emergency. If aircraft have to divert, let them. If aircraft can’t launch, so be it. The “Aggressors” should make every attempt to unexpectedly disrupt and degrade organizational missions, whether it be through attacks against operations, logistics, services, mission support elements, etc.

Highlighting organizational vulnerabilities would be important, but the greatest benefit from this type of training would be an increase in operational readiness.. With adequate resources and a larger footprint, “Aggressor” attacks could make a significant positive impact on the most dynamic and flexible component of cyber-based C4ISR, the Airman. *All Airmen, not just select specialties*, would be better prepared to recognize and respond correctly to attacks on cyber-based C4ISR assets. Airmen would gain confidence in and familiarity with secondary/tertiary C4ISR systems and procedures rehearsed by this paper’s proposed additions to the EM program. Airmen would be better prepared to support national military objectives without losing valuable time adjusting to attacks against cyber-based C4ISR in short-duration high-intensity conflicts.

Conclusion

The above way ahead may seem daunting, but cyber-based C4ISR is an extremely vulnerable center of gravity for the USAF. As noted above, the network's critical requirements are highly susceptible to attack from a number of threats, which include traditional kinetic attack, cyberspace operations, electronic warfare, and anti-satellite weaponry. Potential adversaries are developing and/or already have developed capabilities to exploit these weaknesses, and due to the inherent insecurity and vulnerability of cyber-based C4ISR, the USAF can in no way guarantee the access of cyber-based C4ISR on the battlefield. To mitigate this extremely dangerous situation, the USAF must: 1) convince Airmen the threats are credible, 2) update/create contingency plans, 3) develop and implement an extensive USAF-wide training, exercise, and evaluation program, and 4) expand its existing aggressor program. Only then will the USAF have the potential to meet the nation's strategic military goals and defend its vital national interests across the full spectrum of operations.

Appendix A: Expanded Information on Chinese and Russian Capabilities

China

In the face of the U.S. military's extraordinary victory in Operation DESERT STORM and the disintegration of the Soviet Union,⁷⁴ China began developing cyber attack capabilities as a way to counter technologically superior adversaries starting in the 1990s.⁷⁵ By 2004, China's cyber attack capabilities had matured, backed by cyberwarfare doctrine, a cyberwarfare training program for officers, and integrated cyberwarfare field training.⁷⁶ Moreover, according to the Department of Defense, the Peoples Liberation Army (PLA) has recently created and fielded information warfare units whose sole purpose is to develop and employ methods to attack enemy computer systems and networks (i.e., viruses) while protecting China's networks.⁷⁷ The PLA currently stresses offensive computer network operations (CNO), actively practicing first strike operations against adversaries to ensure "electromagnetic dominance" early in military campaigns.⁷⁸

The most disturbing trend is China's increasingly bold attempts to test new capabilities and isolate its own cyberspace assets from would-be adversaries. For instance, China initiated the largest and most well-known case of cyber-espionage in 2003, when it infiltrated U.S. government, military, and contractor sites.⁷⁹ Government Computer News, an online news agency focusing on the government information technology market, reported that military officials admitted China had downloaded "10 – 20 terabytes of data from the NIPRNET (DOD's Non-Classified IP Router Network)."⁸⁰ Although the NIPRNET it is not a classified system, it stores enormous amounts of sensitive (though unclassified) information⁸¹ tied to operations, logistics, administration, support, etc. The true extent of these, and similar, intrusions is unclear, but they paint a bleak picture for cyberspace. Are the Chinese merely testing their intrusion

capabilities? Or are they also testing U.S. counter-cyber-attack capabilities? Are they gathering and compiling sensitive information to gain an advantage in traditional combat operations? Or did they leave malicious software behind for later use? At a minimum, these intrusions indicate that military information located in cyberspace by no means secure. Worst case, the Chinese have already laid the groundwork to attack USAF cyber-based C4ISR through cyberspace at the time and place of their choosing.

Of course, China's cyber-based attacks are not the only threat to the United States' cyber-based C4ISR. On the contrary, China has been actively pursuing ASAT weaponry to counter the United States' space-based, cyber-based C4ISR infrastructure.⁸² Current satellites do not incorporate robust defensive capabilities, making them highly-susceptible to electronic, kinetic, and/or directed-energy attack...all of which China is perfecting.⁸³ China's first foray into this arena occurred in the late 1990s when it purchased UHF-band jammers for communications satellites from Ukraine.⁸⁴ Since then, the Chinese have likely expanded this capability to include a wide-range of communications and GPS frequencies.⁸⁵ More recently, in January 2007, China demonstrated its newly-developed, yet limited, capability to attack low-Earth orbit satellites.⁸⁶ The Department of Defense has also noted that China is actively attempting to improve their ability to track and identify satellites.⁸⁷ If perfected, the Chinese could combine improved tracking with new ASAT systems to create a formidable offensive space capability.

Russia

As early as 1998, the Russians reportedly conducted a cyber-espionage campaign against the United States.⁸⁸ These intrusions lasted over two years and infiltrated technical defense research data in the Pentagon, NASA, the Energy Department, and multiple private laboratories.⁸⁹ Since then, the Russians have reportedly significantly expanded their

cyberwarfare capabilities. In 2007, citing mounting evidence from U.S. government officials, Russian civilian and military officials, and a Dartmouth University Study in November of 2004, *Jane's Intelligence Digest* indicated the possibility of an extensive Russian cyberwarfare doctrine and offensive capability.⁹⁰ Many believe Russia played a part in recent cyber attacks on Estonia and Georgia.

In addition to its growing cyberwarfare capability, Russia still possesses a growing number of EW weapon systems that could attack U.S. military's cyber-based C4ISR. No doubt building on Cold War-era EW systems, the Russians greatly expanded EW capabilities to support military operations in during the Second Russia-Chechen War.⁹¹ EW warfare forces successfully fielded complexes and portable electronic reconnaissance/suppression and specialized automated jamming systems that allowed its military to "suppress radio, radio-relay, and satellite communication lines and radar and radio navigation systems...[and] to control jamming stations."⁹² Thus, not only has Russian military developed modern EW jamming technologies, it has fielded them in the combat environment.

With regards to ASAT systems, Russia inherited much of the U.S.S.R's Cold War-era space technology and systems. As a result, Russia has access to several proven ASAT systems and a legacy of research and development for others.⁹³ Between 1968 and 1982, the U.S.S.R. conducted numerous successful tests of co-orbital ASAT systems effective up to 1600 kilometers in space, but eventually declared a moratorium on further development due to the Reagan Strategic Defense Initiative.⁹⁴ The U.S.S.R. also extensively researched ground-based laser ASAT systems starting in the 1970s⁹⁵ and fighter aircraft-launched ASAT systems (very similar to the U.S. F-15 launched ASAT system tested in 1985) in the 1980s,⁹⁶ but never operationalized

either system. Russia did, however, preserve one operational, albeit limited, anti-ballistic missile system, the Gorgon Anti-Ballistic Missile Interceptor, that can reach low-flying satellites.⁹⁷

Appendix B: Proposed additions to AFI 10-2501

Course/Event	Audience/Participants	Content	Recurring Frequency (in months)		
			LTM ¹	MTM ¹	HTM ¹
Cyberspace Orientation Course	All Airmen	Very general: definition of cyberspace; cyber-based C4ISR components, capabilities, and vulnerabilities; potential threats; significant attacks to date; generic reporting procedures	N/A	N/A	N/A
Cyberspace Defense Awareness Course	All Airmen	Specific to installation's and organization's mission: cyber-based C4ISR components and capabilities needed to accomplish mission; known/potential threats to components and capabilities; attack recognition; impact of attacks on cyber-based C4ISR...by asset; alternative capabilities; table top scenarios	12 ²	6 ²	3 ²
Installation Computer Network Attack Exercises	As determined by Exercise Program Office...must include 100% organization participation	Realistic simulated large-scale denial, degradation, destruction of multiple computer networks and associated data/hardware (e.g., a malicious computer virus, hacker intrusions, etc.)...include all aspects of base's operations and support	12	6	3
Installation Command, Control, and Communications Attack Exercises	As determined by Exercise Program Office...must include 100% organization participation	Realistic simulated large-scale denial, degradation, destruction of multiple command, control and communications capabilities (e.g., cut in satellite feeds, Internet blackout, telephone blackout)...include all aspects of base's operations and support	12	6	3
Installation Base/Community Infrastructure Attack Exercises	As determined by Exercise Program Office...must include 100% organization participation	Realistic simulated large-scale denial, degradation, destruction of local cyber-based C4ISR infrastructure (e.g., attack on power grids, network nodes, etc.)...include all aspects of base's operations and support	24	12	6
Installation Full Spectrum Cyber-Based C4ISR Attack Exercises	As determined by Exercise Program Office...must include 100% organization participation	Realistic simulated large-scale denial, degradation, destruction of multiple C4ISR capabilities (e.g., attack on local power grid, coupled with malicious computer virus, satellite outages, and telephone outages)...include all aspects of base's operations and support	24	12	6
GCC/FCC/MAJCOM Computer Network Attack Exercises	As determined by GCC/FCC/MAJCOM Exercise Program Office...must include 100% organization participation	Realistic simulated large-scale denial, degradation, destruction of multiple computer networks and associated data/hardware (e.g., a malicious computer virus, hacker intrusions, etc.)...include all aspects of GCC/FCC/MAJCOM's operations and support	12	12	6
GCC/FCC/MAJCOM Command, Control, and Communications Attack Exercises	As determined by GCC/FCC/MAJCOM Exercise Program Office...must include 100% organization participation	Realistic simulated large-scale denial, degradation, destruction of multiple command, control and communications capabilities (e.g., cut in satellite feeds, Internet blackout, telephone blackout)...include all aspects of GCC/FCC/MAJCOM operations and support	12	12	6
GCC/FCC/MAJCOM Infrastructure Attack	As determined by GCC/FCC/MAJCOM	Realistic simulated large-scale denial, degradation, destruction of cyber-based C4ISR	12	12	6

Exercises	Exercise Program Office...must include 100% organization participation	infrastructure (e.g., satellite constellations, Internet cables, satellite relay stations, network nodes, etc.)...include all aspects of GCC/FCC/MAJCOM operations and support			
GCC/FCC/MAJCOM Full Spectrum Cyber-Based C4ISR Attack Exercises	As determined by GCC/FCC/MAJCOM Exercise Program Office...must include 100% organization participation	Realistic simulated large-scale denial, degradation, destruction of multiple C4ISR capabilities (e.g., attack on multiple power grids, coupled with malicious computer virus, satellite outages, and Internet outages, etc.)...include all aspects of GCC/FCC/MAJCOM operations and support	24	24	12

¹LTM = Low Threat Mission, MTM = Medium Threat Mission, HTM = High Threat Mission

²Initially required upon arrival at new duty station (PCS) or temporary duty station (AEF deployment)

Notes

(All notes appear in shortened form. For Full details, see the appropriate entry in the bibliography.)

¹ Quoted in Jim Garamone, “New Military Needs Innovators”

² Office of Management and Budget, “Department of Defense”

³ Department of Defense, *National Defense Budget Estimates*, 205

⁴ Ibid, 205

⁵ Department of Defense, *2008 Enterprise Transition Plan*, 257

⁶ Ibid, 257

⁷ Gates, *National Defense Strategy*, 22

⁸ Joint Publication 1-02, *Dictionary of Military and Associated Terms*, 141

⁹ About.com, “SECRET Internet Protocol”

¹⁰ Jabbour, *50 Cyber Questions*, 4

¹¹ Ibid, 4

¹² Ibid, 4

¹³ Ibid, 4

¹⁴ Ibid, 4

¹⁵ Joint Publication 1-02, *Dictionary of Military and Associated Terms*, 141

¹⁶ Denning, *Information Warfare and Security*, 269

¹⁷ Ibid, 269

¹⁸ Joint Publication 1-02, *Dictionary of Military and Associated Terms*, 181

¹⁹ Kopp, “The Electromagnetic Bomb”

²⁰ Zain, “Cable Damage”

²¹ Mateski, “International, Managing ASATS”

²² Ibid

²³ Ibid

²⁴ Department of Defense, *Annual Report to Congress*, I

- ²⁵ Ibid, I
- ²⁶ Ibid, I
- ²⁷ Billo and Chang, *Cyber Warfare*, 25
- ²⁸ Coleman, “China’s Cyber Forces”
- ²⁹ Department of Defense, *Annual Report to Congress*, 28
- ³⁰ Ibid, 27
- ³¹ Ibid, 28
- ³² *Global Security.org*, “Russian Military Budget”
- ³³ *Global Security.org*, “Nuclear Weapons”
- ³⁴ Reuters, “Russia Restores Bomber Patrols”
- ³⁵ Gonzalez, “Russian, Venezuelan Leaders Tour”
- ³⁶ Mount, “Russian Bombers in Venezuela”
- ³⁷ Coleman, “Russia’s Cyber Forces”
- ³⁸ Thomas, “Information Warfare?”
- ³⁹ *Global Security.org*, “Russia and Anti-Satellite Programs”
- ⁴⁰ Coleman, “Inside DPRK’s Unit 121”
- ⁴¹ Billo and Chang, *Cyber Warfare*, 80
- ⁴² AFP, “North Korea Pursuing Space”
- ⁴³ *Global Security.org*, “North Korea Missiles”
- ⁴⁴ Billo and Chang, *Cyber Warfare*, 60
- ⁴⁵ Ibid, 60
- ⁴⁶ Coleman, “Iranian Cyber Warfare Threat”
- ⁴⁷ Beehner, “Russia-Iran Arms Trade”
- ⁴⁸ Fathi and Broad, “Iran Launches Satellite”
- ⁴⁹ Air Force, “MQ-1 Predator”
- ⁵⁰ Air Force, “MQ-9 Reaper”
- ⁵¹ Air Force, “RQ-4 Global Hawk”
- ⁵² Air Force, “RQ-11 Raven”
- ⁵³ Department of Defense Office of Inspector General, *Contingency Planning for DOD*, 5
- ⁵⁴ Ibid, 8
- ⁵⁵ Ibid, 3
- ⁵⁶ Pace, *National Military Strategy for Cyberspace*, 10
- ⁵⁷ Hansen, “Cyber Flag”, 61
- ⁵⁸ Air Force Instruction (AFI) 10-2501, *Air Force Emergency Management*, 108
- ⁵⁹ Ibid, 7
- ⁶⁰ Ibid, 54
- ⁶¹ Ibid, 86
- ⁶² Air Force Instruction (AFI) 90-201, *Inspector General Activities*, 9
- ⁶³ Air Force Instruction (AFI) 10-2501, *Air Force Emergency Management*, 7
- ⁶⁴ Grill, “Aggressors Prowl for Air Force”

⁶⁵ Ibid

⁶⁶ Ibid

⁶⁷ Lt Col Timothy Franz (Commander, 57th Information Aggressor Squadron, Nellis Air Force Base, NV), interview by the author, 22 March 2009

⁶⁸ Grill, “Aggressors Prowl for Air Force”

⁶⁹ Ibid

⁷⁰ Lt Col Timothy Franz (Commander, 57th Information Aggressor Squadron, Nellis Air Force Base, NV), interview by the author, 22 March 2009

⁷¹ Ibid

⁷² Ibid

⁷³ Jabbour, *50 Cyber Questions*, 11

⁷⁴ Department of Defense, *Annual Report to Congress*, 16

⁷⁵ Billo and Chang, *Cyber Warfare*, 26

⁷⁶ Ibid, 25

⁷⁷ Department of Defense, *Annual Report to Congress*, 28

⁷⁸ Ibid, 28

⁷⁹ Onley, “Red Storm Rising”

⁸⁰ Ibid

⁸¹ Thornburgh, Nathan, “Inside the Chinese Hack Attack”

⁸² Department of Defense, *Annual Report to Congress*, 27-28

⁸³ Ibid, 27-28

⁸⁴ Ibid, 28

⁸⁵ Ibid, 28

⁸⁶ Ibid, 27

⁸⁷ Ibid, 28

⁸⁸ Jane’s Information Group, “Russian Cyber Warfare Capabilities”

⁸⁹ Ibid

⁹⁰ Ibid

⁹¹ Thomas, “Information Warfare”

⁹² Ibid

⁹³ *Global Security.org*, “Russia and Anti-Satellite Programs”

⁹⁴ *Global Security.org*, “Co-Orbital ASAT”

⁹⁵ *Global Security.org*, “Lasers”

⁹⁶ *Global Security.org*, “USSR/CIS Miniature ASAT”

⁹⁷ *Global Security.org*, “Gorgan ABM Interceptor”

Bibliography

- About.com. "SECRET Internet Protocol Router Network." <http://usmilitary.about.com/od/glossarytermss/g/s5586.htm> (accessed 1 February 2009).
- Air Force. "MQ-1 Predator Unmanned Aircraft System." <http://www.af.mil/factsheets/factsheet.asp?fsID=122> (accessed 1 February 2009).
- Air Force. "MQ-9 Reaper Unmanned Aircraft System." <http://www.af.mil/factsheets/factsheet.asp?fsID=6405> (accessed 1 February 2009).
- Air Force. "RQ-4 Global Hawk Unmanned Aircraft System." <http://www.af.mil/factsheets/factsheet.asp?fsID=13225> (accessed 1 February 2009).
- Air Force. "RQ-11 Raven Small Unmanned Aircraft System." <http://www.af.mil/factsheets/factsheet.asp?fsID=10446> (accessed 1 February 2009).
- Air Force Instruction (AFI) 10-2501. *Air Force Emergency Management (EM) Program Planning and Operations*, 24 January 2007 (incorporating change 1, 28 September 2007).
- Air Force Instruction (AFI) 90-201. *Inspector General Activities*, 22 November 2004 (incorporating through change 3, 19 July 2007)
- AFP. "North Korea Pursuing Space Program: State Media." *ABC News*, 7 February 2009. <http://www.abc.net.au/news/stories/2009/02/07/2485144.htm> (accessed 9 February 2009).
- Beehner. "Russia – Iran Arms Trade." *Council on Foreign Relations*, 1 November 2006. <http://www.cfr.org/publication/11869/> (accessed 9 February 2009).
- Billo, Charles and Chang, Welton. *Cyber Warfare: Analysis of the Means and Motivations of Selected Nation States*. Dartmouth College, November 2004 (Revised December 2004). <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf> (accessed 24 January 2009).
- Coleman, Kevin. "China's Cyber Forces." *Defensetech.org*, 8 May 2008. <http://www.defensetech.org/archives/004165.html> (accessed 9 February 2009).
- Coleman, Kevin. "Inside DPRK's Unit 121." *Defensetech.org*, 24 December 2007. <http://www.defensetech.org/archives/003920.html> (accessed 9 February 2009).
- Coleman, Kevin. "Iranian Cyber Warfare Threat Assessment." *Defensetech.org*, 23 September 2008. <http://www.defensetech.org/archives/004432.html> (accessed 9 February 2009).
- Coleman, Kevin. "Russia's Cyber Forces." *Defensetech.org*, 27 May 2008. <http://www.defensetech.org/archives/004200.html> (accessed 25 January 2009)
- Denning, Dorothy E. *Information Warfare and Security*. Boston, MA: Addison-Wesley, 1999.
- Department of Defense. *2008 Enterprise Transition Plan: ETP*. Washington, D.C.: Government Printing Office, 30 September 2008.
- Department of Defense. *Annual Report to Congress on the Military Power of the People's Republic of China 2008*. Washington, D.C.: Government Printing Office, 2008.
- Department of Defense. *National Defense Budget Estimates for FY 2009*. Washington, D.C., Government Printing Office, March 2008 (as amended through October 2008).
- Department of Defense Office of Inspector General. *Contingency Planning for DOD Mission-Critical Information Systems*. DODIG Report D-2008-047. Washington, D.C.: Government Printing Office, 5 February 2008
- Fathi, Nazila and Broad, William J. "Iran Launches Satellite in a Challenge for Obama." *The New York Times*, 3 February 2009. <http://www.nytimes.com/2009/02/04/world/middleeast/04iran.html> (accessed 9 February 2009).
- Garamone, Jim. "Bush Says New Military Needs Innovators." Department of Defense.

- <http://www.defenselink.mil/news/newsarticle.aspx?id=45830> (accessed on 23 November 2008)
- Gates, Robert M. *National Defense Strategy*. Department of Defense. Washington, D.C.: Government Printing Office, June 2008.
- Global Security.org*. "Co-orbital ASAT." <http://www.globalsecurity.org/space/world/russia/coorb.htm> (accessed 9 February 2009).
- Global Security.org*. "Gorgan ABM Interceptor." <http://www.globalsecurity.org/space/world/russia/gorgan.htm> (accessed 9 February 2009).
- Global Security.org*. "Lasers." <http://www.globalsecurity.org/space/world/russia/lasers.htm> (accessed 9 February 2009).
- Global Security.org*. "North Korea Missiles." <http://www.globalsecurity.org/wmd/world/dprk/missile.htm> (accessed 9 February 2009).
- Global Security.org*. "Nuclear Weapons." <http://www.globalsecurity.org/wmd/world/russia/nuke.htm> (accessed 24 January 2009).
- Global Security.org*. "Russia and Ant-Satellite Programs." <http://www.globalsecurity.org/space/world/russia/asat.htm> (accessed 25 January 2009).
- Global Security.org*. "Russian Military Budget." <http://www.globalsecurity.org/military/world/russia/mo-budget.htm> (accessed 24 January 2009).
- Global Security.org*. "USSR/CIS Miniature ASAT." <http://www.globalsecurity.org/space/world/russia/mini.htm> (accessed 9 February 2009).
- Gonzales, Maria C. "Russian, Venezuelan Leaders Tour Fleet." *CNN.com*, 27 November 2008. <http://www.cnn.com/2008/WORLD/americas/11/27/venezuela.russia/index.html> (accessed 24 January 2009).
- Grill, MSgt Eric M. "Aggressors Prowl For Air Force Information." *Air Force Link*, 27 February 2009. <http://www.af.mil/news/story.asp?id=123137445> (accessed 20 March 2009).
- Hansen, Andrew P. *Cyber Flag: A Realistic Cyberspace Training Construct*. Maxwell AFB, AL: Air University Press, March 2008.
- Jabbour, Dr. Kamal T. *50 Cyber Questions Every Airmen Can Answer*. Wright Patterson Air Force Base, OH: Air Force Research Laboratory, 2008.
- Jane's Information Group. "Russian Cyberwarfare Capabilities." *Jane's Intelligence Digest*, 15 June 2007. http://search.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jid/history/jid2007/jid70129.htm@current&pageSelected=allJanes&keyword=russia%20cyber&backPath=http://search.janes.com/Search&Prod_Name=JID& (accessed 24 January 2009).
- Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Washington D.C.: Government Printing Office, 12 April 2001 (as amended through 17 October 2008).
- Kopp, Carlo. "The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction." *Global Security.org*. <http://www.globalsecurity.org/military/library/report/1996/apjemp.htm> (accessed 10 February 2009).
- Mateski, Mark. "International, Managing ASATS: The Threat to US Space." *Jane's Intelligence Review*, 1 May 1999. http://search.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jir/history/jir99/jir00246.htm@current&pageSelected=allJanes&keyword=Russian%20ASAT&backPath=http://search.janes.com/Search&Prod_Name=JIR& (accessed 25 January 2009).
- Mount, Mike. "Russian Bombers in Venezuela Amid Tension with U.S." *CNN.com*, 11

- September 2008. <http://www.cnn.com/2008/WORLD/americas/09/11/russia.venezuela/index.html> (accessed on 24 January 2009).
- Office of Management and Budget. "Department of Defense." Washington D.C., <http://www.whitehouse.gov/omb/budget/fy2005/defense.html> (accessed 24 January 2009).
- Onley, Dawn S. "Red Storm Rising." *Government Computer News*, 17 August 2006. <http://gcn.com/Articles/2006/08/17/Red-storm-rising.aspx> (accessed 24 January 2009).
- Pace, General Peter, Chairman of the Joint Chiefs of Staff. National Military Strategy for Cyberspace Operations (NMS-CO). Washington D.C: Government Printing Office, December 2006.
- Reuters. "Russia Restores Bomber Patrols." *CNN.com*, 17 August 2007. <http://www.cnn.com/2007/WORLD/europe/08/17/russia.airforce.reut/index.html> (accessed 24 January 2009)
- Thomas, Timothy L. "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?" For Leavenworth, KS: Foreign Military Studies Office, 2002. <http://fmso.leavenworth.army.mil/documents/iwchechen.htm> (accessed 28 January 2009).
- Thornburgh, Nathan. "Inside the Chinese Hack Attack." *Time*, 25 August 2005. <http://www.time.com/time/nation/article/0,8599,1098371,00.html> (accessed on 24 January 2009).
- Zain, Asma A. "Cable Damage Hits 1.7m Internet Users in UAE." *Khaleej Times Online*, 5 February 2008. http://www.khaleejtimes.com/DisplayArticle.asp?xfile=data/theuae/2008/February/theuae_February155.xml§ion=theuae (accessed 25 January 2009).